IT Security and Requirements at CUMC

Students using Columbia University UNI accounts, University and Medical Center networks, email, and other institutional technical resources must comply with University policies and security requirements. These are put in place to protect devices and data in an increasingly complex, mobile environment where individuals are held accountable for the release of sensitive information, whether it was done intentionally or not.

Acceptable Use of Network and Computing Resources

Columbia's Acceptable Use of IT Resources Policy is presented and must be agreed to when activating your Columbia UNI account. It is every individual's responsibility to know and adhere to its requirements as well as all applicable policies found at [http://policylibrary.columbia.edu](http://policylibrary.columbia.edu). They include:

- Prohibition of the use of University resources for illegal or criminal purposes, copyright infringement, excessive use or malicious intent.
- Properly securing your computers, devices and accounts to safeguard against hacking or other malicious use. You are ultimately responsible for the traffic traveling through your equipment.
- Adequately protecting data according to its level of sensitivity through the use of strong passwords, encryption, proper disposal and other approved methods.

The Medical Center has additional responsibility to protect sensitive data covered by federal HIPAA regulations and the HI-TECH act. A full list of CUMC related requirements and guidelines is online at [http://www.cumc.columbia.edu/it/policy](http://www.cumc.columbia.edu/it/policy). They include:

- Completion of required online Security and Privacy training by all new students, and on an annual basis thereafter: [http://www.cumc.columbia.edu/it/security_training.html](http://www.cumc.columbia.edu/it/security_training.html)
- All computers must run current antivirus and antispyware programs with recent updates installed.
- All computers must run operating system updates to insure that critical vulnerabilities are patched.
- Automatic email forwarding to outside addresses cannot be configured on institutional email accounts.
- Computers and other devices that store or access sensitive data must use approved forms of encryption. See recommended programs at [http://www.cumc.columbia.edu/it/howto/encrypt/recommend.html](http://www.cumc.columbia.edu/it/howto/encrypt/recommend.html)
- No networking devices (routers, wireless access points, etc.) that provide Network Address Translation (give out IP addresses on the campus networks) can be set up unless approved by a school’s Dean and done in conjunction with CORE Resources, the group that manages CUMC’s networks.

How can I comply with these requirements?

1. Be aware of IT security practices and employ them in day to day use. Not taking the time to review policies or understand how to use security programs work does not excuse an individual from penalties. This is particularly important for anyone entering a field where they will be working with patient and personally identifiable information; even if you are not yet accessing patient data, we urge you to take the time to become familiar with encryption and other security programs that will be required.

2. Be vigilant. Don’t assume that because others seem to be operating fine without using best security practices, it’s okay for you to do it too. The network is monitored for excessive use and unusual activity; accounts that access sensitive and institutional information are often logged and audited for security.

3. Understand that using an institution’s IT resources requires a balance of convenience and security. Those managing the resources do their best to implement security measures that don’t adversely affect the work you need to do, but will still require some standardization and advance approval for non-standard use.

Continued on other side
Account Security

Your IDs and passwords are the keys to a great amount of personal information about you and your work.

**Keep your password secret.** It is against Columbia University policy to share your password. You must never give it to anyone, not even a spouse or close friend. You must also use strong passwords that contain letters, numbers, and special characters on all of the systems that you log in to, and not use the same password for outside accounts.

**Do not set automatic forwarding on your email account.** CUMC must comply with federal regulations protecting confidential and sensitive data such as protected health (PHI) and personally identifiable information (PII). To avoid its release, accidental or otherwise, institutional email cannot be automatically forwarded to an external account including Gmail, iCloud, Yahoo, etc.

**Do not save passwords in a program, and log out of public systems completely.** Enter your password every time you open program, even if you think no one else has access to your computer. Log out when you’re done to make sure someone else can’t access the information in your account.

**Avoid sending confidential information via email even when the messages are encrypted.** There’s no telling what a recipient will do with that information, whether by accident or with malicious intent.

**Use a screensaver password** - but do not use your email/UNI password for your screensaver. To set one in Windows go to Control Panel - User Accounts..., select the account you’re using and the Create a password link. On Mac OS X, open System Preferences and select Users & Groups, then Change Password.

System Security

Below are a list of measures that must be taken to fully protect your computer, data, and personal information:

**Avoid opening web site links from an email or instant message.** Be wary of messages with links that you weren’t already expecting. Opening a web page from an email message can be just as dangerous as opening an attachment. The past years have seen a huge rise in "Phishing", where a web site, email or instant message seems authentic but is actually an attempt to steal personal identity information.

**Use Symantec Endpoint** - [http://cuit.columbia.edu/symantec](http://cuit.columbia.edu/symantec). Symantec is free for Columbia students and staff. Set virus definitions to update automatically and daily, as new malicious programs are constantly being released.

**Keep your operating system patched and up to date.** New vulnerabilities in operating systems are regularly discovered and exploited. To prevent viruses or worse, use a built-in update program and set it to update automatically: Windows Update for Windows and Software Update for Mac OS X are two examples. You can learn how to use these programs at [http://cuit.columbia.edu/cuit/it-security-resources](http://cuit.columbia.edu/cuit/it-security-resources). If you use an OS other than Windows or Mac, get on a mailing list such as CERT Alerts ([https://www.us-cert.gov/ncas/alerts](https://www.us-cert.gov/ncas/alerts)) to receive information about updates.

**Protect your mobile devices.** Never leave a laptop, tablet or smartphone unattended. They are easily stolen even when locked; cable laptop locks can be cut off and removed. Columbia provides the laptop security program Phone-Home at no cost via [http://cuit.columbia.edu/pc-phonehome](http://cuit.columbia.edu/pc-phonehome). It will attempt to locate your laptop if stolen; be sure to read the FAQs linked on the site before installing for full information on how it operates. Other mobile devices must adhere to policies found at [https://secure.cumc.columbia.edu/cumcit/secure/policy/phone.html](https://secure.cumc.columbia.edu/cumcit/secure/policy/phone.html)

**Use Hardware Encrypted USB Keys and set encryption on mobile devices.** Data on your computer and other media such as USB keys/flash drives, and compact and DVD discs can be easily encrypted in a way that is transparent to you. This prevents information from being discovered if the computer or media are stolen or lost, and is a vital consideration for anyone affiliated with CUMC whether or not you regularly work with sensitive information. Encrypted USB keys can be purchased at the Service Desk on the 2nd floor of the Hammer building.

**Back up your data regularly and securely.** Data loss from corruption, system failure, or loss or theft of a device can happen without warning. Windows and Macintosh systems have automatic backup features that can insure you have recent copies of your work; just make sure you are backing up to secured, encrypted media whenever the backups contain sensitive information. [http://www.cumc.columbia.edu/it/getting_started/backup.html](http://www.cumc.columbia.edu/it/getting_started/backup.html)

For more information, please see [http://www.cumc.columbia.edu/it/safety](http://www.cumc.columbia.edu/it/safety) or contact us with specific questions.